PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32

A1

(11) International Publication Number: WO 00/13368

(43) International Publication Date: 9 March 2000 (09.03.00)

(21) International Application Number: PCT/US99/18824

(22) International Filing Date: 27 August 1999 (27.08.99)

(30) Priority Data:
09/144,043 31 August 1998 (31.08.98) US

(71)(72) Applicant and Inventor: BORGERS, Frederick, J. [US/US]; 105 Mill Valley, Colleyville, TX 76034 (US).

(74) Agent: PERDUE, Mark, D.; Zisman Law Firm, 200 Renaissance Place, 714 Jackson, Dallas, TX 75202 (US).

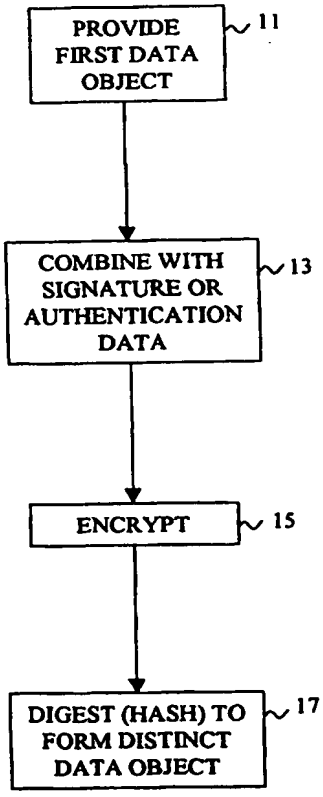
(81) Designated States: CA, IL, IN, JP, KR, MX, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

(57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time–stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to providing authentication of digital data, such as document or other data files or objects. More particularly, the present invention relates to methods of securely appending or otherwise incorporating a digital signature or indicia of authenticity into a data object.

BACKGROUND OF THE INVENTION AND BACKGROUND ART

There have been several prior attempts to digitally "sign," "notarize," or otherwise authenticate a digital data object such as a text document. Generally speaking, one drawback to the storage of, for instance, digital document files, is that it can be difficult to establish whether the version retrieved or transmitted is the identical document originally stored or created. A "digital signature" or "notary" is a common nomenclature for an attempt to provide indicia of authenticity of the digital data.

One such method is found in U.S. Patent Number 5,022,080, June 4, 1991, to Durst et al., which discloses a method of digitally notarizing a document comprising the steps of hashing the document, transmitting the digest (or result of the hash) to a trusted third party, where the digest is combined with a time-stamp, and then encrypting the combination to produce a "digitally notarized" document. All that is required to authenticate the document is the key to the encryption technique. Thus, simply by "breaking the code" the authenticity indicia or the underlying data object can be altered

or tampered with.

Other solutions complicate this basic scheme to render it more difficult to break the code successfully. For instance, U.S. Patent Number 5,373,561, December 13, 1994 to Haber et al., periodically re-encrypts the signature data to take advantage of ever-increasing computational power and advances in encryption, which also render the authentic document more susceptible to alteration, decryption, or tampering as time passes. However, if the user neglects to "update" the encryption, the advantage is lost.

A need exists, therefore, for a method of digitally authenticating a data object that is not susceptible to future tampering, yet is sufficiently simple as to be implemented in a practical and efficient manner.

DISCLOSURE OF THE INVENTION

It is a general object of the present invention to provide a method of providing a data object that can ve verified or authenticated reliably, with minimal risk of tampering.

This and other objects of the present invention are achieved by associating or combining a data object, such as a document file, with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated or digested from the combination of encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data.

According to the preferred embodiment of the present invention, the generation of the distinct data object is achieved using a hashing algorithm, such as SHA-1.

According to the preferred embodiment of the present invention, the signature or authentication data is provided by a trusted third party. The data object transmitted to the third party may be a digest or hash of the data object to preserve the confidentiality of the data object.

According to the preferred embodiment of the present invention, the encryption step is achieved by a symmetric encryption algorithm.

According to the preferred embodiment of the present invention, the authenticity of the original data object is confirmed by reproducing the distinct data object by identically encrypting a data object identical to the original, generating another distinct data object, and comparing the second and first distinct data objects for identity.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a high-level flow chart depicting the steps of the method according to the preferred embodiment of the present invention, and more particularly the steps of proving a data object with authentication or signature data.

Figure 2 is a block diagram schematically depicting a portion of the method of **Figure 1** according to the preferred embodiment of the present invention.

Figure 3 is a high-level flow chart illustrating the steps of the method according to the preferred embodiment of the present invention, and more particularly of the steps of authenticating a data object provided with authentication data.

Figure 4 is a block diagram schematically depicting a portion of the method of **Figure 3** according to the preferred embodiment of the present invention.

MODE(S) FOR CARRYING OUT THE INVENTION

Referring now to the Figures, and specifically to Figure 1, a high-level flow-chart depicts the basic steps of a portion of the method according to the present invention. First, at block 11, a first data object or item is provided by a user or customer of the method. The data object or item could be a document, drawing, image file, or any item or segment of data that the user desires to provide with the ability to be authenticated or verified in the future.

At block 13, the data object is combined or associated with signature or authentication data. The signature or authentication may include the time of creation of the data object, the name of the author of the object, predetermined characters indicating the origin of the object, or virtually any other data the user desires to serve as evidence of authenticity of the underlying data object. According to the preferred embodiment of the present invention, the authentication data is a "time stamp" that comprises, for instance, the time and date from the "Atomic Clock" maintained by the United States Naval Observatory (e.g., 22:13.02; 4 April 1998). The signature or authentication data is appended, concatenated, or otherwise conventionally combined or associated with the data object. As discussed in greater detail with reference to Figure 2, the time stamp or other signature or authentication data is provided by a trusted third party, perhaps the vendor of the method, who also keeps meticulous records of the method used to combine or associate the data object with signature or authentication data.

Next, at block 15, the combination of the data object and signature or authentication data is encrypted using conventional symmetric secret-key, asymmetric

public-key techniques or other combining techniques which use a key known only to the trusted third party. The encryption technique could be as simple as appending or concatenating a selected, random text or character string to the data object. For maximum security, it is preferable that the trusted third-party employ secret-key techniques and maintain a record of the encryption technique along with any secret-keys, for future use in authentication of the data object. The preferred encryption method or algorithm is RC5.

Finally, at block 17, the encrypted data object is digested or hashed using a hash routine to generate a distinct data object. A hash routine generates a data string that is characteristic of the underlying data object that is subjected to the hash routine. The preferred hashing algorithm is SHA-1. There are several hashing routines or algorithms, such as SHA-1, that are suitable for use in the method according to the present invention. All of these hashing routines or algorithms share the following characteristics:

- the underlying data object cannot be reproduced from the hashed data string (it is a one-way or irreversible process);
- the routine produces a data string of fixed length; and
- the routine will not yield the same data string for two different data objects.

Hashing is sometimes referred to as a method of encryption, but this is inaccurate: the very essence of encryption is that it can be decrypted or the process reversed. Hashing, by its very nature, is not reversible. According to the preferred embodiment of the present invention, the hashing or digesting step may comprise application of a single hashing algorithm or routine to the encrypted data object and signature data.

Alternatively, the hashing step may comprise multiple applications of the same or different hashing algorithms.

The result of the hashing step is a distinct data object that has characteristics of both the underlying data object and the signature or authentication data. The distinct data object may be appended to or separate from the underlying data object. The distinct data object and the signature or authentication data is transmitted, along with the original data object to a recipient party to permit the recipient party to later confirm the authenticity of the original data object and/or the combination of the data object and the signature or authentication data.

Figure 2 is a block diagram depicting elements and relationships between entities performing the steps of the method according to the present invention. According to the preferred embodiment of the present invention, the encryption and hashing steps are performed on the user's computer 19 which may be a personal computer, a client/server workstation, terminal for a mainframe or minicomputer or the like. The signature or authentication data is provided by a trusted third party 21, who also provides the encryption and hashing algorithms and keeps a record of the encryption or combining techniques and any secret keys for use in future authentication. Alternatively, the encryption and hashing algorithms are resident on and maintained by user's system 19.

According to one embodiment of the invention, the original data object is hashed and then sent to the trusted third party 21 to preserve the confidentiality of the original data object. In this embodiment, the trusted third party performs the encryption and hashing or digesting steps and returns the resulting distinct data object and authentication

data to user 19 to associate with or combine with the original data object.

Communication between user 19 and trusted third party 21 is accomplished in a number of ways: through modem line, T1 line, frame relay link, or cable modem, or http protocol (each with appropriate security). Trusted third party 21 maintains records of any encryption keys, the encryption technique and hashing algorithm(s) for future use by the party that later performs authentication of the document.

Figure 3 is a high-level flow chart depicting the steps of the authentication portion of the method according to the present invention. To authenticate the data object, an original copy, block 31, of the data object, identical to the first, is combined with signature or authentication data, at block 33. The original copy of the data object and signature or authentication data can be provided by the originator, or can be kept by the trusted third party along with the encryption and/or hashing algorithms. After the copy of the original data object is combined with the authentication or signature data, the combinations is encrypted in an identical fashion to the original, at block 35. At block 37, the resulting encrypted data object is then hashed or digested identically to the first, and the resulting distinct data object compared with the original data object (the result of block 17 in Figure 1) and the two are compared for identity. If the two are identical, the underlying data object (or the copy) is thus verified or authenticated. If not identical, the data object or copy is not authenticated and cannot be trusted (i.e., the copy or document purporting to be original has been altered and is not identical to the first or the authentication data has been altered).

Figure 4 is a block diagram depicting elements and relationships between entities

performing the steps of the authentication portion of the method according to the present invention. According to the preferred embodiment of the present invention, the authentication steps are performed by a trusted party, perhaps the vendor of the method as the recipient party 25 using information provided by the trusted third party, the originator or user, or a combination of the two. The distinct data objects are input to a comparator or a computer algorithm operable to compare data for identity. The output of the comparator verifies the authenticity (or lack thereof).

According to the preferred embodiment of the present invention, the method is performed using software resident on the document or data object originator's computer. The encryption and digesting occurs on the trusted third party's computer with the input and results being communicated to and from the trusted third party as described above. The recipient of the "authenticated" data object can request verification through the trusted third party, depending upon which of the parties maintains the requisite encryption technique, hashing algorithm, combination method, and any encryption keys.

The method according to the present invention provides an improved method of digitally signing or otherwise authenticating digital data objects. Because the hashing or digesting step is one-way or irreversible, the encrypted portion of the "signature" is not susceptible to unauthorized decryption, even by marked advances in computational power. Because of this advantage, the trusted third party or vendor must keep scrupulous records of the encryption or combining techniques, hashing methods and encryption keys employed in providing the signature or authentication data.

The invention has been described with reference to preferred embodiments thereof.

It is thus not limited, but is susceptible to variation and modification without departing from the scope and spirit of the invention, which is defined by the claims, which follow.

CLAIMS

1. A method of securely associating signature data with other data, the method comprising the steps of:

associating a data object with signature data;

encrypting both the data object and the signature data; and

generating a distinct data object from the encrypted data object and signature data, the distinct data object having characteristics determined by the data object and the signature data.

2. The method according to claim 1 further comprising the step of:

delivering the distinct data object and signature data to a recipient party.

3. The method according to claim 2, further comprising the step of:

validating the distinct data object and signature data combination by:

associating a second data object, identical to the first, with the signature data;

encrypting the second data object and the signature data using an encryption method identical to that employed in encrypting the first data object and the signature data;

generating a second distinct data object from the encrypted second data object and the signature data using an method identical to that employed in generating the distinct data object; and

comparing the distinct and second distinct data objects for identity.

4. The method according to claim 1, wherein the signature data is provided by a trusted party.

5. The method according to claim 1, wherein the encrypting step is performed using a symmetric data encryption technique.

6. The method according to claim 1, wherein the step of generating the distinct data object is performed using a hash routine.

7. A method of providing a time-stamp for a data object comprising the steps of:

generating a distinct value for the data object;

associating signature data with the distinct value to produce a signed data object;

encrypting the signed data object; and

generating a second distinct value from the encrypted signed data object, the second distinct data object having characteristics of the encrypted signed data object.

8. The method according to claim 7 further comprising the step of:

delivering the second distinct data object and signature data to a recipient party.

9. The method according to claim 8, further comprising the step of:

validating the second distinct data object and signature data combination by:

generating a third distinct value, identical to the distinct value;

associating a second signature data, identical to the first, with the third distinct value to produce a second signed data object; and

encrypting the second signed data object using an encryption method identical to that employed in encrypting the first signed data object;

generating a fourth distinct value from the encrypted second signed data object using method identical to that employed in generating the second distinct value; and

comparing the fourth distinct value and second distinct value for identity.

10. The method according to claim 7, wherein the signature data is provided by a trusted party.

11 The method according to claim 7, wherein the encrypting step is performed using a symmetric data encryption technique.

12. The method according to claim 7, wherein the step of generating the distinct value is performed using a hash routine.

13. A method of providing a time-stamp for a data object comprising the steps of:

generating a distinct value for the data object by performing a hash routine on the data object;

associating a time-stamp with the distinct value to produce a time-stamped data object;

encrypting the time-stamped data object; and

generating a second distinct value from the encrypted time-stamped data object by performing a hash routine on the encrypted time-stamped data object.

14. The method according to claim 13 further comprising the step of:

delivering the second distinct data object and time-stamp to a recipient party.

15. The method according to claim 13, further comprising the step of:

validating the second distinct data object and time-stamp combination by:

generating a third distinct value, identical to the distinct value;

associating a identical time-stamp with the third distinct value to produce a second time-stamped data object

encrypting the second time-stamped data object using the identical encryption method;

generating a forth distinct value from the encrypted second time-stamped data object; and

comparing the fourth distinct value and second distinct value for identity.

16. The method according to claim 13, wherein the time stamp is provided by a trusted party.

17. The method according to claim 13, wherein the encrypting step is performed using

a symmetric data encryption technique.

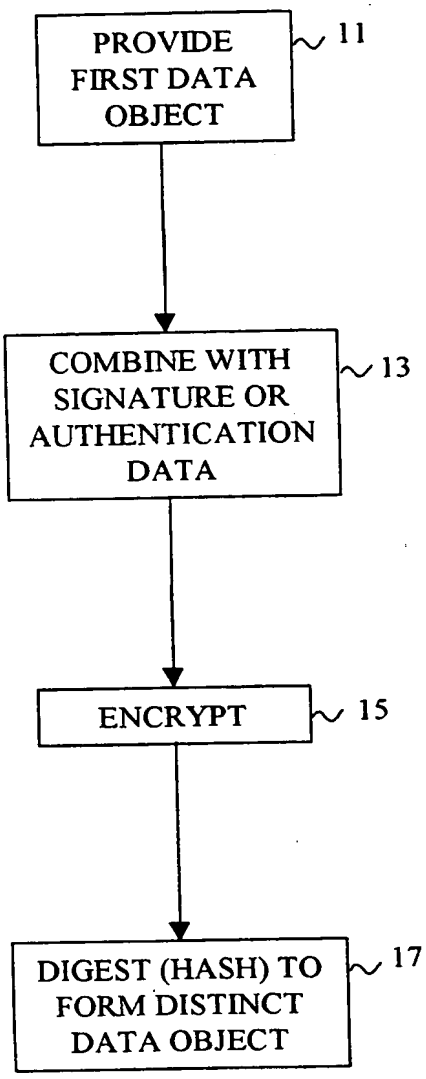

PROVIDE FIRST DATA OBJECT
11
COMBINE WITH SIGNATURE OR AUTHENTICATION DATA
13
ENCRYPT
15
DIGEST (HASH) TO FORM DISTINCT DATA OBJECT
17

FIG. 1

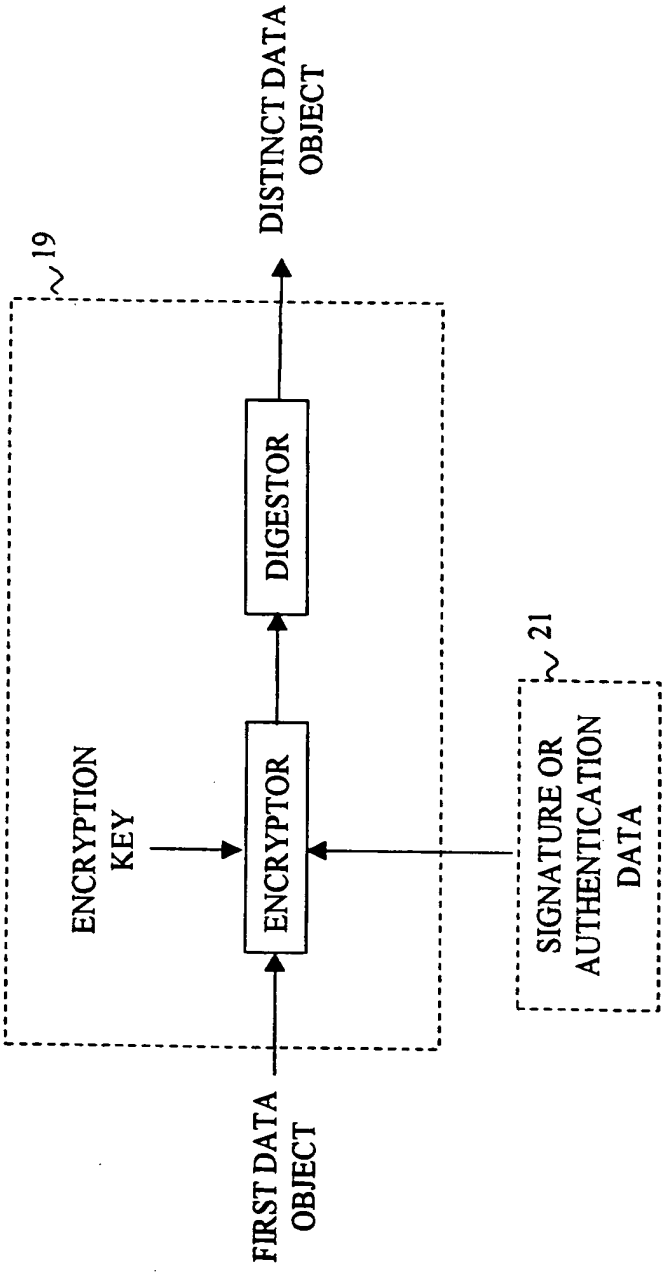


FIG. 2

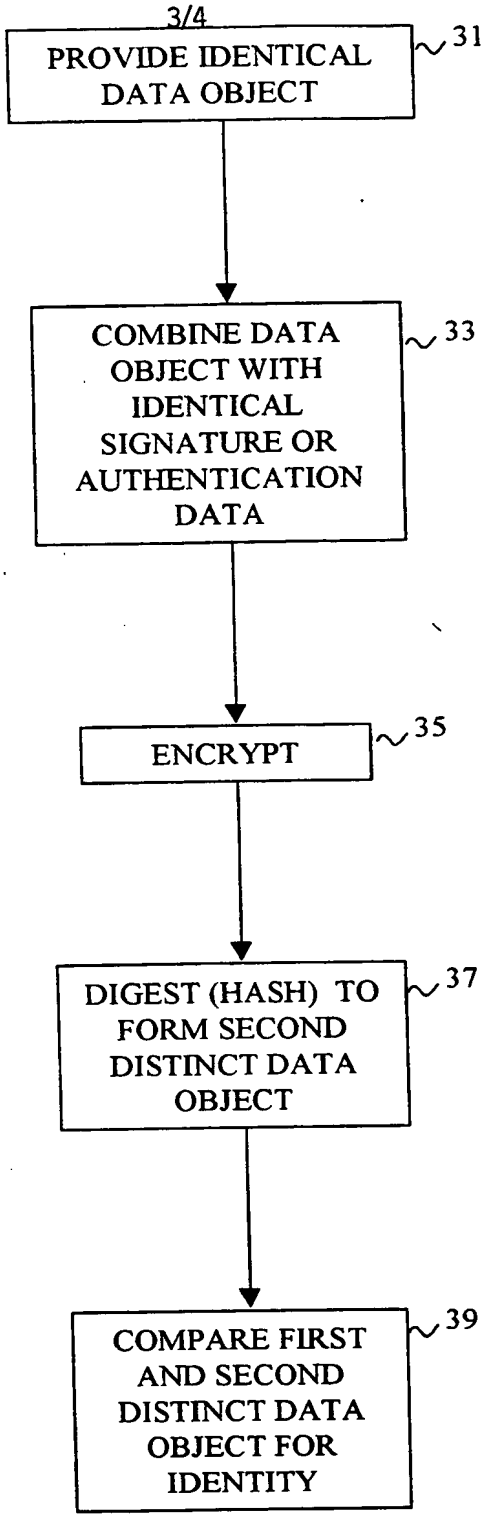


FIG. 3

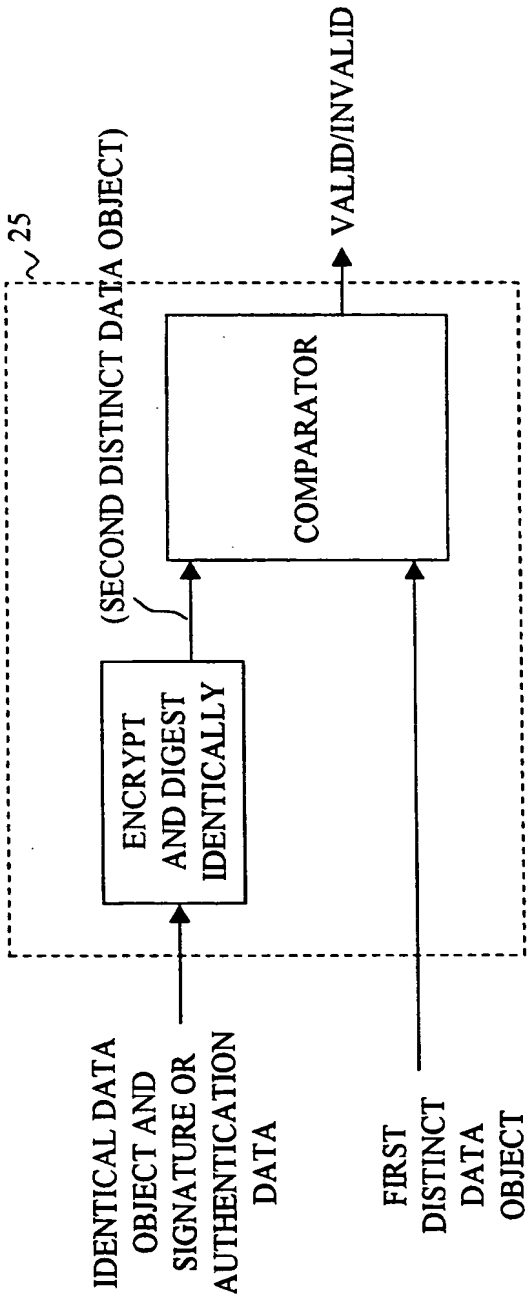


FIG. 4

INTERNATIONAL SEARCH REPORT

Inter ›nal Application No
PCT/US 99/18824

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	MITCHELL C ET AL: "CCITT/ISO standards for secure message handling" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, MAY 1989, USA, vol. 7, no. 4, pages 517-524, XP000007972 ISSN: 0733-8716 page 520, column 2 -page 522, column 1 ---	1-17
X	SWAIN N: "Getting the message safely. Security and X.400 systems" COMPUTER FRAUD & SECURITY BULLETIN, MARCH 1992, UK, pages 10-15, XP000862948 ISSN: 0142-0496 page 13, column 1, paragraph 3 -page 14, column 1, paragraph 1 --- -/--	1-17

[X] Further documents are listed in the continuation of box C

[X] Patent family members are listed in annex.

Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 December 1999	21/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 99/18824

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of the relevant passages	Relevant to claim No
X	US 5 022 080 A (DURST ROBERT T ET AL) 4 June 1991 (1991-06-04) cited in the application column 3, line 65 -column 6, line 54	1-17
X	US 5 373 561 A (HABER STUART A ET AL) 13 December 1994 (1994-12-13) cited in the application column 2, line 38 -column 6, line 44	1-17
X	US 5 638 446 A (RUBIN AVIEL D) 10 June 1997 (1997-06-10) column 3, line 49 -column 6, line 20	1-17

1

INTERNATIONAL SEARCH REPORT

...nformation on patent family members

Inter ...nal Application No
PCT/US 99/18824

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5022080 A	04-06-1991	CA 2043533 A,C	01-12-1992
		JP 6014018 A	21-01-1994
		EP 0516898 A	09-12-1994
US 5373561 A	13-12-1994	AU 670166 B	04-07-1996
		AU 5670694 A	19-07-1994
		CA 2151590 A,C	07-07-1994
		EP 0676109 A	11-10-1995
		JP 8504965 T	28-05-1996
		WO 9415421 A	07-07-1994
US 5638446 A	10-06-1997	NONE	

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/32

A1

(11) International Publication Number: WO 00/13368

(43) International Publication Date: 9 March 2000 (09.03.00)

(21) International Application Number: PCT/US99/18824

(22) International Filing Date: 27 August 1999 (27.08.99)

(30) Priority Data:
09/144,043 31 August 1998 (31.08.98) US

(71)(72) Applicant and Inventor: BORGERS, Frederick, J. [US/US]; 105 Mill Valley, Colleyville, TX 76034 (US).

(74) Agent: PERDUE, Mark, D.; Zisman Law Firm, 200 Renaissance Place, 714 Jackson, Dallas, TX 75202 (US).

(81) Designated States: CA, IL, IN, JP, KR, MX, SG, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

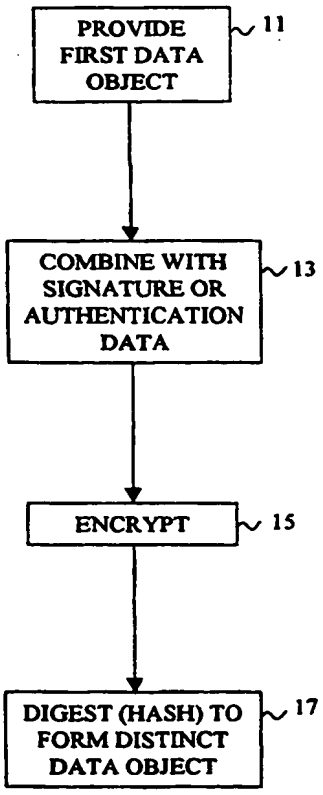
Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

(57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



*(Referred to in PCT Gazette No. 21/2000, Section II)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

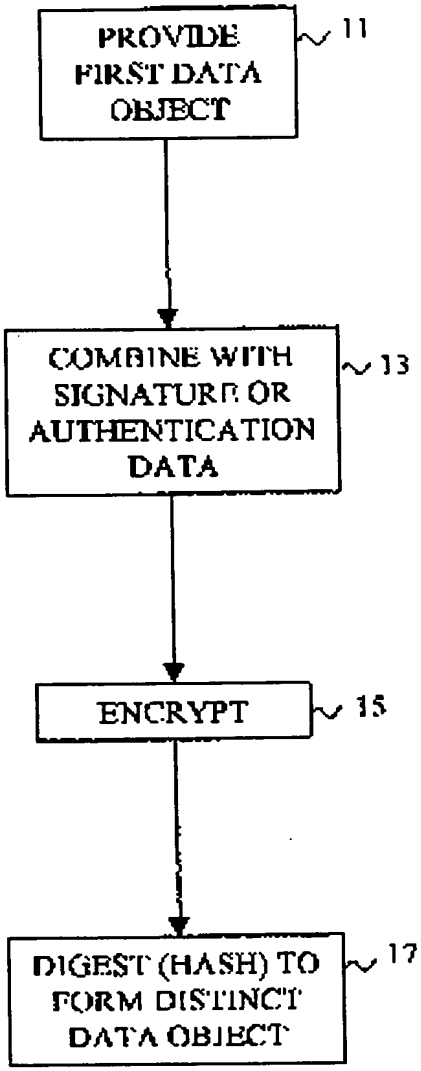

PROVIDE FIRST DATA OBJECT
11
COMBINE WITH SIGNATURE OR AUTHENTICATION DATA
13
ENCRYPT
15
DIGEST (HASH) TO FORM DISTINCT DATA OBJECT
17

FIG. 1

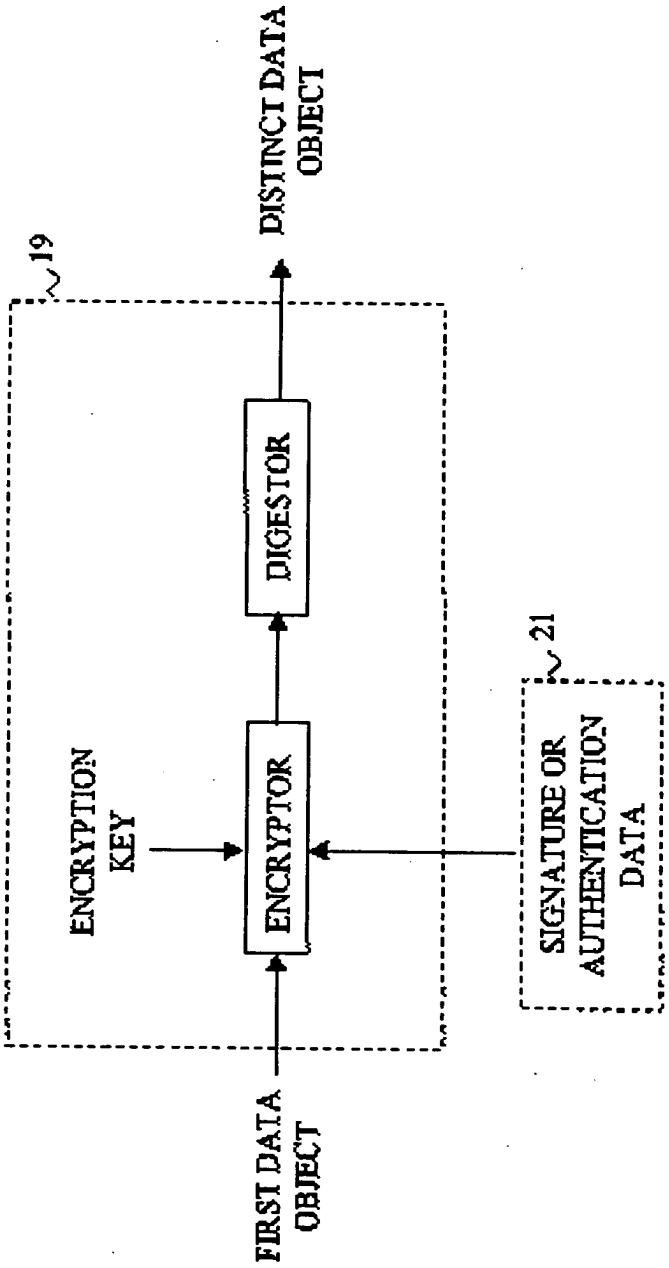


FIG. 2

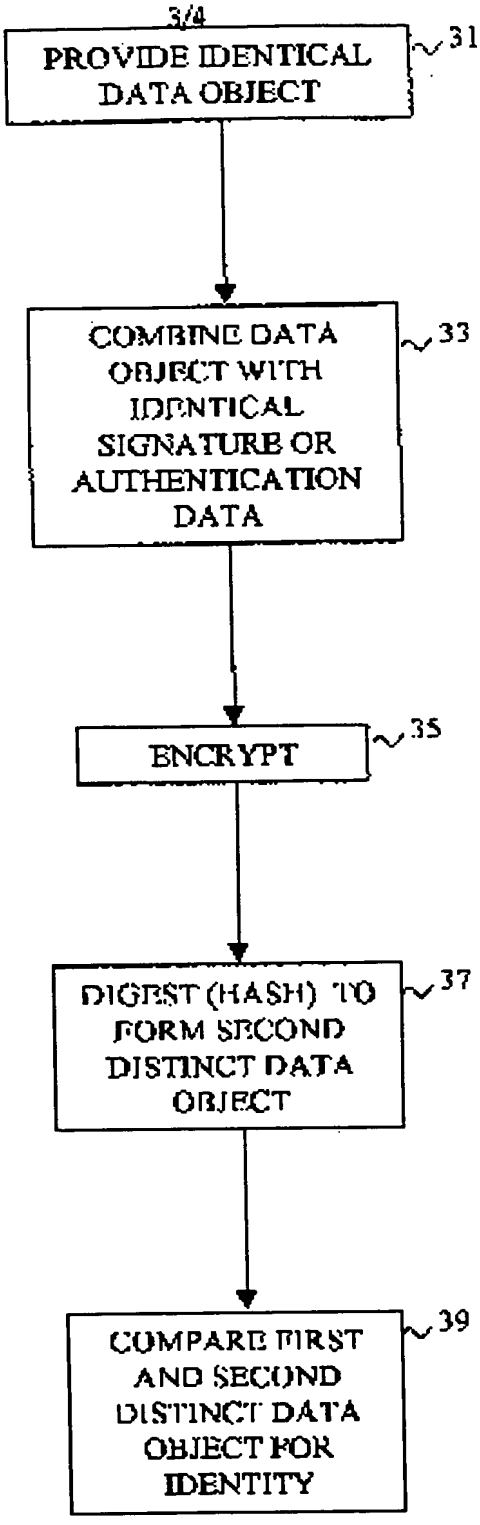

PROVIDE IDENTICAL DATA OBJECT
31
COMBINE DATA OBJECT WITH IDENTICAL SIGNATURE OR AUTHENTICATION DATA
33
ENCRYPT
35
DIGEST (HASH) TO FORM SECOND DISTINCT DATA OBJECT
37
COMPARE FIRST AND SECOND DISTINCT DATA OBJECT FOR IDENTITY
39

FIG. 3

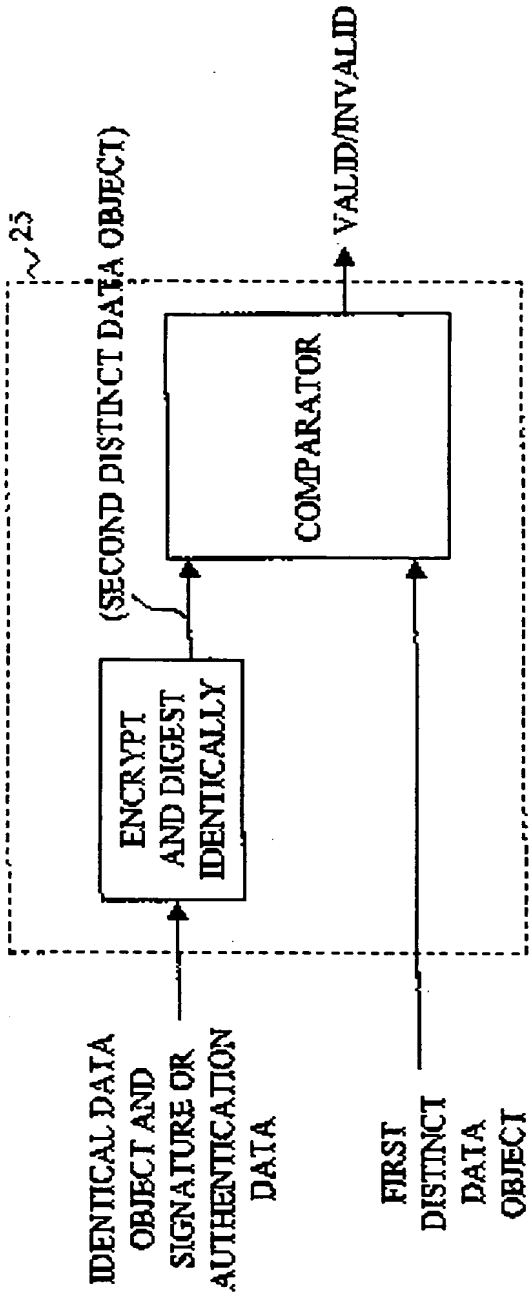


FIG. 4